— AUS（アルテミス・ユーザ・サポート）便り 2020/09/28号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Windowsのドメインコントローラに重大な脆弱性「Zerologon」…8月リリース済みパッチの適用を

https://japan.zdnet.com/article/35159600/
https://jp.techcrunch.com/2020/09/20/2020-09-19-homeland-security-emergency-alert-critical-windows-bug/
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-1472

このニュースをザックリ言うと･･･

- 9月11日(現地時間)、オランダのセキュリティ企業Secura社より、Windows Serverにおいて修正された重大な脆弱性について注意喚起が出されています。

- 「Zerologon」と名付けられた脆弱性はWindows Serverのドメインコントローラ(DC)機能に存在し、悪用により、DCサーバーのみならず、DCが管理するドメイン上の任意のPCをも乗っ取りが可能になるとされています。

- 既に攻撃コードが出回っているとされ、米国土安全保障省(DHS)も当該脆弱性を「緊急」レベルの危険度に認定しています。

- Microsoftでは8月にリリースされた月例のセキュリティパッチで脆弱性に対応しており、DCサーバーにパッチが適用されているか確認するよう強く呼び掛けられています。

AUS便りからの所感等

- 脆弱性は厳密にはWindows PC(あるいはその他デバイス)とDCとの通信プロトコルに存在するものですが、ともあれ、特に中規模以上の企業・組織においては、Active Directoryにより社内PCにおけるユーザーアカウント等を管理しているケースが多く、脆弱性の影響を受ける可能性が高いとみられます。

- Microsoftでは脆弱性の対策を二段階に分けて行うとしており、8月のWindowsに対するパッチを一段階目とし、Windows以外を対象とする二段階目の対策を2021年1～3月のパッチリリースにて行う予定としています。

- Windows Serverと互換性のあるファイル共有機能やDC機能等も提供する「Samba」についても同様の脆弱性が発現する(ファイルサーバーとしてのみ使用の場合は影響しない)とのことで、LinuxサーバーとSambaでDCを構築している場合にもアップデートもしくは回避策の実行が必要となることにご注意ください。

ZDNet Japan

「Windows Server」の脆弱性「Zerologon」--その深刻性が明らかに

Catalin Cimpanu（ZDNet.com）翻訳校正：編集部　2020-09-15 12:39

Microsoftは8月の月例パッチで、今までに同社に報告されたもののなかで最も深刻度の高い部類に入る脆弱性に対処した。この脆弱性が悪用された場合、企業ネットワーク上でドメインコントローラーとして機能している「Windows Server」を簡単に乗っ取られてしまう可能性がある。

共通脆弱性識別子「CVE-2020-1472」が割り当てられたこの脆弱性は、8月の月例セキュリティパッチで対処された。同脆弱性は、ドメインコントローラーに対するユーザー認証プロトコル「Netlogon」に存在している、権限昇格を引き起こす脆弱性と説明されている。

この脆弱性は10段階の深刻度スコアで10と評価されているものの、詳細は公開されていなかったため、ユーザーやIT管理者は今までその本当の恐ろしさを知ることができなかった。

しかし、オランダのセキュリティ企業Secuaのチームは現地時間9月11日、この謎多き脆弱性の正体をようやく明らかにするとともに、CVE-2020-1472について詳しく説明する技術レポートを同社ブログ上で公開した。

●預金不正引き出し、PayPay等でも…銀行口座からの即時振替サービス一時休止

https://www.watch.impress.co.jp/docs/news/1277259.html
https://www.itmedia.co.jp/mobile/articles/2009/16/news056.html
https://paypay.ne.jp/notice/20200915/06/
https://paypay.ne.jp/notice/20200915/07/
https://www.jp-bank.japanpost.jp/news/2020/news_id001543.html

このニュースをザックリ言うと・・・

- 9月上旬に報じられた「ドコモ口座」の悪用による銀行預金不正引き出し事件(AUS便り 2020/09/14号参照)について、他の決済サービスでも同様の事案が発生し、銀行預金からの即時口座振替を停止する事態となっています。

- 9月15日(日本時間)、PayPayより、2020年1月～8月にゆうちょ銀行において17件、被害額約141万円分の不正利用が発生していたこと(9月にゆうちょ銀行利用時の本人確認導入後は不正利用は発生していないとのことです)、また同行や地方銀行等について口座新規登録およびチャージを一時停止していることが発表されています。

- 同日にはゆうちょ銀行より、PayPayの他にLINE Pay・メルペイ・Kyashへの不正出金が確認されたことと、これらに加えPayPal・楽天Edy等を含めた複数の決済サービスについて口座新規登録およびチャージの一時停止が発表されています。

- また被害額について、ドコモ口座側発表(9月23日付、 http://ngt.idc.nttdocomo.co.jp/20200923_00.pdf)では総額2,776万円、ゆうちょ銀行側発表(9月23日付、 https://www.jp-bank.japanpost.jp/aboutus/press/2020/pdf/pr200924_4.pdf)では総額約6,000万円とされています。

AUS便りからの所感

- 適当な口座番号と暗証番号だけで(その他の認証・本人確認要素がなくても)決して見過ごせない割合で悪用が可能であったことが示されており、たとえ推測されにくい暗証番号の設定をユーザー側に呼び掛けたとしても、仕組みがサービス側で改められない限り、根本的な問題の解決とはなり得ないとみられます。

- 決済サービス各社等では、登録の際にスマートフォンのカメラで本人の顔と免許証等の本人確認書類を撮影してもらう、いわゆる「eKYC」の導入を進めており、今回の事件を受けたユーザー側からも、利用したいサービスにこういった本人確認手段が導入されているか等を今後注視されていく可能性があるでしょう。

Impress Watch

PayPay、ゆうちょ銀行の不正利用は8カ月で141万円。9月以降は発生せず

臼田勤哉　2020年9月15日 23:53

PayPayは15日、ゆうちょ銀行における不正利用が、2020年1月以降の8カ月間で17件、141万5,141円と発表した。いずれもPayPayの全額補償制度の対象となり、補償申請があった被害者には補償に向けた対応を実施している(一部は全額補償済み)。

なお、PayPayでは9月に本人確認(eKYC)をゆうちょ銀行で全導入。以降は不正利用は発生していないという。

●コロナ禍でサーバダウン狙う「DDoS攻撃」が3倍に… Kaspersky調査

https://www.itmedia.co.jp/news/articles/2009/18/news149.html
https://www.kaspersky.co.jp/about/press-releases/2020_vir18092020

このニュースをザックリ言うと・・・

- 9月18日(日本時間)、セキュリティベンダーのKaspersky社より、2020年第2四半期(4～6月)のDDoS攻撃に関する調査結果レポートが発表されました。

- 同社セキュリティ製品によりブロックされたDDoS攻撃件数は、2019年第2四半期の316.67%に上ったとしています。

- 例年のDDoS攻撃は企業や組織の繁忙期となる第1四半期(1～3月)に集中し、第2四半期には減少する傾向にある中、2020年第1四半期(1～3月)が2019年第2四半期の302.08%であったのに比べて増加しており、例年と異なる傾向にあるとされています。

- Kaspersky社では「新型コロナウイルスの世界的な大流行で、夏の休暇の外出機会が減り、オンラインサービスを利用する時間が増えたため」としています。

AUS便りからの所感

- 上記の他、攻撃対象となった国の割合トップ10では中国66.02%、アメリカ19.32%、香港6.34%、以下順に南アフリカ・シンガポール・オーストラリア・ベトナム・インド・日本・韓国となっており、日本は0.23%で初めてトップ10入りしています。

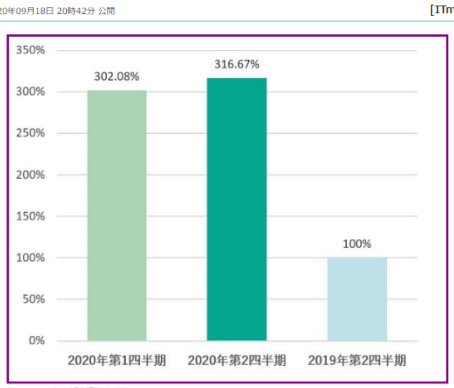
- トップ10全体で見れば6～10位はいずれも微々たる割合に見えるものの、第1四半期から割合が増加したのは中国・ベトナムそして日本となっており、コロナ禍の劇的な解消が見られない現時点では、特に年末となる第4四半期において、全体的な攻撃件数、日本がターゲットとされる割合、そしてDDoS以外にも様々な攻撃がさらに増えている可能性も皆無ではないでしょう。

- 今年前半には早急にテレワーク等への対応が求められたきらいもありましたが、その体制を少なからず維持することを鑑みるならば、一旦構築したシステムについてセキュリティの点検と整理・整備が行われているべき時期と言えます。

ITmedia NEWS

コロナ禍でサーバダウン狙う「DDoS攻撃」が3倍にカスペルスキー調査

2020年09月18日 20時42分 公開　[ITmedia]



カスペルスキーが公表したグラフ